REMARKS

Please reconsider the subject application in view of the following remarks.

Claims 1-20 are pending in the application, with claims 1, 15 and 18 being the independent claims.

Claim 1 stands rejected under 35 USC 103(a) as being unpatentable over "IBM Cryptolopes, Super Distribution and Digital Rights Measurement," (Kaplan) in view of U.S. Patent No. 6,021,491 (Renaud). Claims 2-17 stand rejected under 35 USC 103 as being unpatentable over Kaplan in view of Renaud, and further in view of the article "Cryptology for Digital TV Broadcasting" (Macq). Claims 18-20 stand rejected under 35 USC 103 as being unpatentable over Kaplan in view of Renaud and Schneier and further in view of Macq. Applicant traverses these rejections.

Independent Claim 1

In independent claim 1, the claimed invention recites a method for managing access to a scrambled event of a service provider featuring, *inter alia*, receiving in a device, in response to user selection of an event from a list of events, a digital signature and an encrypted message associated with the selected event. The digital signature is encrypted with a first key and the encrypted message is encrypted with a second key different from the first key. The encrypted message includes a descrambling key and event information. The method of claim 1 also includes authenticating in the device a source of the digital signature and the encrypted message associated with the selected event by decrypting the digital signature in response to receiving the digital signature and the encrypted message. Upon authenticating the source, the encrypted message is decrypted in the device to obtain the descrambling key. The method also includes receiving in the device the selected event from the service provider, the selected event being scrambled using the descrambling key for preventing unauthorized access to the selected event, and descrambling in the device the selected event using the descrambling key.

Many of these features are not taught or suggested by Kaplan and Renaud, whether those documents are taken alone or in proper combination.

In the Response to Arguments section of the Office Action, the Examiner indicates that the arguments submitted in the last Response were not persuasive because several claim features argued in that Response were not in the claims. Applicant disagrees, because all of the features underlined by the Examiner on pages 2 and 3 of the Office Action were, and still are, in the claims by virtue of the amendments made in the Response filed May 29, 2007. The Examiner's contention that those features are not in claim 1 is perplexing.

Nevertheless, the Examiner also asserts that all features of claim 1 are shown in the combination of Kaplan and Renaud. Specifically, the Examiner is taking the position that Kaplan teaches all features of claim 1, except "authenticating in the device a source of the digital signature and the encrypted message."

As best understood, Kaplan teaches a cryptographic envelope (cryptolope) containing, *inter alia*, parts (text or images) encrypted using a document key. The document keys for accessing the encrypted information are encrypted using a master key and are stored in a key record within the cryptolope. When a user desires to obtain the information contained in the cryptolope, he initiates a transaction with, for example, a website. The process of purchasing is described on page 7 of Kaplan, and includes creating a buy request cryptolope containing a Bill of Materials, Terms and Conditions for getting the information, and the key records, as well as user credentials. The buy request cryptolope is then sent to a clearing center that verifies the transaction, and thereafter decrypts the key files and re-encrypts the document keys under the public key of a module of the user. These encrypted document keys are then sent back to the user, where they are decrypted and used for accessing the encrypted information.

The Office Action is asserting that the "encrypted part" of Kaplan's cryptolope corresponds to the "encrypted message" of claim 1. If this is the case, the encrypted part of Kaplan does not "comprise a descrambling key and event information," as required by claim 1. The "encrypted part" of Kaplan is understood to be the ultimate content to be viewed (or listened to, etc.). Moreover, if the encrypted part of Kaplan corresponds to the claimed encrypted message, what part of Kaplan corresponds to the event? If the cryptolope corresponds to the event, the cryptolope is not scrambled as required by claim 1, and a descrambling key is not included in the encrypted part. Kaplan is deficient in teaching all features of claim 1.

Renaud is cited only for teaching verification of digital signatures and data generally, and therefore does not correct these deficiencies of Kaplan.

Thus, the combination of Kaplan and Renaud fails to teach all features of the invention of claim 1. Favorable reconsideration and withdrawal of the rejection of claim 1 thus are requested.

Independent Claims 15 and 18

Independent claims 15 and 18 recite methods for managing access between a device having a smart card coupled thereto and a service provider. The method of claim 15 includes receiving an electronic program guide from a guide provider, the guide having a message and a digital signature associated with each event in the guide, the message being encrypted using a public key of the smart card and the digital signature being created using a private key of the guide provider.

The method of claim 18 includes receiving an electronic program guide from a guide provider, the guide having a digital certificate and a separate message corresponding to each event in the guide. Each of the digital certificates is encrypted using a first private key of the guide and the separate message is encrypted using a public key of the smart card and having an associated digital signature created using a second private key of the guide.

Many of these features are not taught or suggested by Kaplan, Renaud and Marq, whether taken alone or in proper combination.

Specifically, and for reasons similar to those described above with respect to claim 1, Kaplan is not understood to teach a message and a digital signature associated with each event in a guide, with the message encrypted, as recited in claim 15, nor is it understood to teach or suggest a digital certificate and a separate message corresponding to each event in the guide, with the message being encrypted. Because the Examiner is equating the "encrypted part" of Kaplan with the claimed encrypted message, the rejection must fail, because while the encrypted part of Kaplan is encrypted, it is not decrypted to obtain event information and a symmetric key, as required by claims 15 and 18.

Moreover, the combination of these references is not understood to teach or suggest decrypting a message associated with/corresponding to an event in a guide to obtain event

information and a symmetric key and then using the symmetric key to descramble a scrambled event, as also recited in claims 15 and 18.

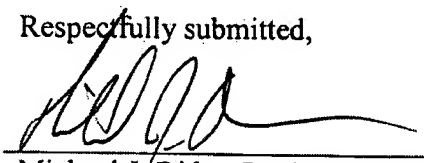
For the foregoing reasons, Applicant submits that independent claims 1, 15, and 18 are allowable over the cited patent documents. Favorable reconsideration and withdrawal of the rejections of these claims are requested.

The remaining claims depend from the independent claims. These claims are believed to be allowable by virtue of this dependency, and for reciting other patentable features of Applicant(s) invention. Favorable and independent consideration of the dependent claims respectfully are requested.

Applicant submits that claims 1-20 of this application stand in condition for allowance. Accordingly, reconsideration and an early notice of allowance are respectfully solicited.

If necessary, Applicant's representative may be reached by telephone at (585) 232-6500 with any questions regarding this application. All written correspondence should continue to be forwarded to the address of record for this application.

Respectfully submitted,



Michael J. Didas, Registration No. 55,112
Customer Number 23387
HARTER SECREST & EMERY LLP
1600 Bausch & Lomb Place
Rochester, New York 14604
Telephone: 585-232-6500
Fax: 585-232-2152